

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:

Eiji HASEGAWA, et al.

Application No.:

Group Art Unit:

Filed: February 24, 2004

Examiner:

For: INFORMATION PROCESSING APPARATUS

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-372374

Filed: October 31, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: February 24, 2004

By: 

J. Randall Beckers  
Registration No. 30,358

1201 New York Ave, N.W., Suite 700  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2003年10月31日

出願番号  
Application Number: 特願2003-372374

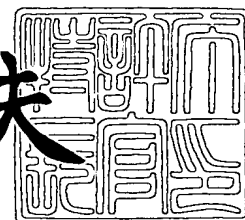
[ST. 10/C]: [JP 2003-372374]

出願人  
Applicant(s): 富士通株式会社

2004年 2月16日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特2004-3009678



【書類名】 特許願  
【整理番号】 0395318  
【提出日】 平成15年10月31日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G06F 9/06  
【発明者】  
    【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社  
                                内  
    【氏名】 長谷川 英司  
【発明者】  
    【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社  
                                内  
    【氏名】 本田 文雄  
【特許出願人】  
    【識別番号】 000005223  
    【氏名又は名称】 富士通株式会社  
【代理人】  
    【識別番号】 100078868  
    【弁理士】  
    【氏名又は名称】 河野 登夫  
    【電話番号】 06-6944-4141  
【国等の委託研究の成果に係る記載事項】 平成15年度、通信・放送機構、「PCなど  
        オープンアーキテクチャーデジタル放送受信機に対応する権利保  
        護システムの研究開発」委託研究、産業活力再生特別措置法第3  
        0条の適用を受ける特許出願  
【手数料の表示】  
    【予納台帳番号】 001889  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9705356

**【書類名】 特許請求の範囲****【請求項 1】**

第 1 の記憶手段と、  
該第 1 の記憶手段に書き込まれたプログラムを実行する CPU と、  
セキュアモジュールと、  
暗号化されたプログラムを記憶する第 2 の記憶手段と  
を有する情報処理装置において、  
前記第 2 の記憶手段は、複数に分割されたプログラムを記憶しており、  
前記 CPU は、前記第 2 の記憶手段に記憶されたプログラムを前記セキュアモジュール  
へ転送すべくしてあり、

前記セキュアモジュールは、前記第 2 の記憶手段に記憶されたプログラムを受け取る手段と、受け取ったプログラムを実行可能な状態へ復帰させる手段と、前記 CPU が実行する順序で、実行可能な状態へ復帰されたプログラムを前記第 1 の記憶手段に書き込む手段と、前記 CPU により実行されたプログラムを、実行終了後に前記第 1 の記憶手段から削除する手段とを備えることを特徴とする情報処理装置。

**【請求項 2】**

前記セキュアモジュールは、分割されたプログラムに対する実行要求信号を受信したか否かを判断する手段を備え、該手段が実行要求信号を受信したと判断した場合、受け取ったプログラムを実行可能な状態へ復帰させるものであることを特徴とする請求項 1 記載の情報処理装置。

**【請求項 3】**

前記セキュアモジュールは、分割されたプログラムについて、前記第 1 の記憶手段にプログラム実行前に常駐させるプログラムか、実行されるまで前記メモリに書き込まれないプログラムかを識別する情報を記憶する手段を備えることを特徴とする請求項 1 又は 2 に記載の情報処理装置。

**【請求項 4】**

第 1 の記憶手段と、  
該第 1 の記憶手段に書き込まれたプログラムを実行する CPU と、  
セキュアモジュールと、  
暗号化されたプログラムを記憶する第 2 の記憶手段と  
を有する情報処理装置において、  
前記 CPU は、前記第 2 の記憶手段に記憶されたプログラムを前記セキュアモジュール  
へ転送すべくしてあり、

前記セキュアモジュールは、前記第 2 の記憶手段に記憶されたプログラムを受け取る手段と、受け取ったプログラムを複数に分割する手段と、分割されたプログラムを実行可能な状態へ復帰させる手段と、前記 CPU が実行する順序で、実行可能な状態へ復帰されたプログラムを前記第 1 の記憶手段に書き込む手段と、前記 CPU により実行されたプログラムを、実行終了後に前記第 1 の記憶手段から削除する手段とを備えることを特徴とする情報処理装置。

**【請求項 5】**

前記第 2 の記憶手段は、記憶されたプログラムに対応付けて、プログラムの分割に関する情報を記憶しており、前記セキュアモジュールは、前記プログラムの分割に関する情報に基づいて受け取ったプログラムを複数に分割すべくしてあることを特徴とする請求項 4 記載の情報処理装置。

**【請求項 6】**

第 1 の記憶手段と、  
該第 1 の記憶手段に書き込まれたプログラムを実行する CPU と、  
セキュアモジュールと、  
暗号化されたプログラムを記憶する第 2 の記憶手段と  
を有する情報処理装置において、

前記第 1 の記憶手段は、複数に分割されたプログラムを実行前に常駐させてあり、

前記第 2 の記憶手段は、分割されたプログラムを実行プログラムとして呼び出す呼び出しプログラムを記憶してあり、前記第 2 の記憶手段に記憶された呼び出しプログラムを前記セキュアモジュールへ転送すべくしてあり、

前記セキュアモジュールは、前記第 2 の記憶手段に記憶された呼び出しプログラムを受け取る手段と、受け取った呼び出しプログラムを実行可能な状態へ復帰させる手段と、前記 CPU が分割されたプログラムを実行する順序で、対応する実行可能な状態へ復帰された呼び出しプログラムを前記第 1 の記憶手段に書き込む手段と、前記 CPU により実行された呼び出しプログラムを、実行終了後に前記第 1 の記憶手段から削除する手段とを備えることを特徴とする情報処理装置。

【請求項 7】

前記第 1 の記憶手段は、分割されたプログラム間の呼び出し関係を指定する情報であるリンク情報をさらに記憶してあり、前記セキュアモジュールは、前記リンク情報に基づいて分割されたプログラムを実行する順序を検出すべくしてあることを特徴とする請求項 6 記載の情報処理装置。

【書類名】明細書

【発明の名称】情報処理装置

【技術分野】

【0 0 0 1】

本発明は、プログラムを実行する場合に、悪意の第三者による解析を困難にする情報処理装置に関する。特に、情報処理装置に着脱可能に実装され、プログラムを実行する際のセキュリティに関する処理を実行するセキュアモジュールを用いた情報処理装置に関する。

【背景技術】

【0 0 0 2】

近年、ブロードバンドインターネットに代表される常時接続環境が普及し、悪意ある第三者による不正なプログラムの実行、更新等に対する安全性を確保する技術が着目されている。特に、パーソナルコンピュータ（Personal Computer：以下「PC」という。）はオープンなアーキテクチャを有し、PC上で実行されるプログラムは、オペレーティングシステム（以下、OSという。）又はプロセッサに準拠した形式のプログラムコードとして記述される。したがって、基本的には誰でもPC上のメインメモリの内容を確認し、理解することができるため、安全性を確保することは困難であるという問題点があった。

【0 0 0 3】

斯かる問題点を解決すべく、従来は、実行されるプログラムを難読化又はセキュア化する技術を使用し、例えばプログラムのロジックを複雑にすることにより逆解析を困難にする、プログラムを暗号化する、プログラムをメモリに動的に書き込みながら実行する（特許文献1参照）等の対策が取られている。

【0 0 0 4】

また、特許文献2には、オープンなアーキテクチャを有する情報処理装置に、外部モジュールとして、内部に解析又は参照することが不可能な領域を有するセキュアモジュールを組み合わせ、該セキュアモジュールによりプログラムをメモリに書き込む技術が開示されている。斯かる技術を用いる場合、プログラムが記憶媒体に記憶されている間は、外部から解析又は参照することが不可能な情報を使用してプログラムを暗号化しており、第三者による内容の解析を防止している。また、プログラムを書き込んだメモリをプロセッサと独立動作するセキュアモジュールにより監視することにより、実行するプログラムの安全性をより高めている。

【特許文献1】特開平11-232103号公報

【特許文献2】特開2003-198527号公報

【発明の開示】

【発明が解決しようとする課題】

【0 0 0 5】

しかし、実行されるプログラムを難読化又はセキュア化する技術を使用する方法では、いかにプログラムを難読化又はセキュア化しようと、最終的にはオープンなアーキテクチャ上で動作するプログラムとして記述することには変わりはない。したがって、メモリに書き込まれたロードモジュールを逆解析し、周知であるオープンなアーキテクチャに沿って命令、データ等を調査することで、実行されるプログラムの内容を解析することは可能であり、第三者による不正な攻撃を防ぐことはできない。

【0 0 0 6】

また、セキュアモジュールを用いてプログラムをメモリに書き込んで実行する方法を使用する場合であっても、プロセッサが実行可能な形式でプログラムがメモリに書き込まれることには変わりはなく、メモリの内容をイメージコピーし、イメージコピーに基づいてメモリの内容を解析することで、実行されるプログラムの内容を解析することは可能である。

【0 0 0 7】

本発明は斯かる事情に鑑みてなされたものであり、プログラムを実行する場合に、悪意

ある第三者による逆解析を困難にし、実行するプログラムの安全性を高めることができる情報処理装置を提供することを目的とする。

【課題を解決するための手段】

【0008】

上記目的を達成するために第1発明に係る情報処理装置は、第1の記憶手段と、該第1の記憶手段に書き込まれたプログラムを実行するCPUと、セキュアモジュールと、暗号化されたプログラムを記憶する第2の記憶手段とを有する情報処理装置において、前記第2の記憶手段は、複数に分割されたプログラムを記憶しており、前記CPUは、前記第2の記憶手段に記憶されたプログラムを前記セキュアモジュールへ転送すべくしてあり、前記セキュアモジュールは、前記第2の記憶手段に記憶されたプログラムを受け取る手段と、受け取ったプログラムを実行可能な状態へ復帰させる手段と、前記CPUが実行する順序で、実行可能な状態へ復帰されたプログラムを前記第1の記憶手段に書き込む手段と、前記CPUにより実行されたプログラムを、実行終了後に前記第1の記憶手段から削除する手段とを備えることを特徴とする。

【0009】

第1発明に係る情報処理装置では、暗号化されたプログラムを複数に分割して記憶しておき、分割されたプログラム単位で実行可能な状態へ復帰させ、実行する順序で第1の記憶手段（例えばメモリ）へ書き込む。実行が完了したプログラムは、第1の記憶手段上から削除する。これにより、プログラム実行時にプログラムのすべての内容が第1の記憶手段上に書き込まれていることがなく、実行時には部分的なプログラムのみが第1の記憶手段へ書き込まれていることから、悪意ある第三者が第1の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム全体の内容を取得することができないことからプログラム内容を解析することができず、実行するプログラムの安全性を確保することが可能となる。

【0010】

また、第2発明に係る情報処理装置は、第1発明において、前記セキュアモジュールは、分割されたプログラムに対する実行要求信号を受信したか否かを判断する手段を備え、該手段が実行要求信号を受信したと判断した場合、受け取ったプログラムを実行可能な状態へ復帰させるものであることを特徴とする。

【0011】

第2発明に係る情報処理装置では、分割されたプログラムに対する実行要求信号を受信してから、要求対象である分割されたプログラムを実行可能な状態へ復帰させて第1の記憶手段（例えばメモリ）へ書き込む。これにより、実行要求が出された時点で初めて第1の記憶手段へプログラムが記憶されることから、実行要求が出されるまではプログラムの一部は第1の記憶手段へ書き込まれておらず、外部から第1の記憶手段の内容を参照した場合であってもプログラム全体の内容を把握することは困難であり、実行するプログラムの安全性をより高めることが可能となる。

【0012】

また、第3発明に係る情報処理装置は、第1発明又は第2発明において、前記セキュアモジュールは、分割されたプログラムについて、前記第1の記憶手段にプログラム実行前に常駐させるプログラムか、実行されるまで前記メモリに書き込まれないプログラムかを識別する情報を記憶する手段を備えることを特徴とする。

【0013】

第3発明に係る情報処理装置では、分割されたプログラムの重要性、秘匿性等に基づいて、第1の記憶手段（例えばメモリ）に常時書き込んでおいてもよいプログラムであるか否かを識別する情報を付与する。これにより、重要性、秘匿性等の低いプログラムは第1の記憶手段上に常時書き込んでおき、重要性、秘匿性等の高いプログラムは実行時のみ第1の記憶手段に書き込むことで、必要なプログラムのみ実行の安全性を高めることができ、安全性を確保するための処理によるプログラムのオーバーヘッドを低減することが可能となる。

**【0014】**

また、第4発明に係る情報処理装置は、第1の記憶手段と、該第1の記憶手段に書き込まれたプログラムを実行するCPUと、セキュアモジュールと、暗号化されたプログラムを記憶する第2の記憶手段とを有する情報処理装置において、前記CPUは、前記第2の記憶手段に記憶されたプログラムを前記セキュアモジュールへ転送すべくしてあり、前記セキュアモジュールは、前記第2の記憶手段に記憶されたプログラムを受け取る手段と、受け取ったプログラムを複数に分割する手段と、分割されたプログラムを実行可能な状態へ復帰させる手段と、前記CPUが実行する順序で、実行可能な状態へ復帰されたプログラムを前記第1の記憶手段に書き込む手段と、前記CPUにより実行されたプログラムを、実行終了後に前記第1の記憶手段から削除する手段とを備えることを特徴とする。

**【0015】**

第4発明に係る情報処理装置では、セキュアモジュールが、記憶されている暗号化されたプログラムを複数に分割し、分割したプログラム単位で実行可能な状態へ復帰させ、実行する順序で第1の記憶手段（例えばメモリ）へ書き込む。実行が完了したプログラムは、第1の記憶手段上から削除する。これにより、プログラム実行時にプログラムのすべての内容が第1の記憶手段上に書き込まれていることがなく、実行時には部分的なプログラムのみが第1の記憶手段へ書き込まれていることから、悪意ある第三者が第1の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム全体の内容を取得することができないことからプログラム内容を解析することができず、実行するプログラムの安全性を確保することが可能となる。

**【0016】**

また、第5発明に係る情報処理装置は、第4発明において、前記第2の記憶手段は、記憶されたプログラムに対応付けて、プログラムの分割に関する情報を記憶してあり、前記セキュアモジュールは、前記プログラムの分割に関する情報に基づいて受け取ったプログラムを複数に分割すべくしてあることを特徴とする。

**【0017】**

第5発明に係る情報処理装置では、セキュアモジュールは、受け取る分割されたプログラムに対応付けて記憶されているプログラムの分割に関する情報、例えば分割単位に基づいてプログラムを分割し、分割したプログラム単位で実行可能な状態へ復帰させる。これにより、記憶されているプログラムの分割に関する情報に基づいて適正にプログラムを分割することができ、例えば分割単位が不適切であることにより、多くの分割されたプログラムが第1の記憶手段に書き込まれる状態が生じることを回避し、悪意ある第三者が第1の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム内容の解析をより困難にすることができ、実行するプログラムの安全性を確保することが可能となる。

**【0018】**

また、第6発明に係る情報処理装置は、第1の記憶手段と、該第1の記憶手段に書き込まれたプログラムを実行するCPUと、セキュアモジュールと、暗号化されたプログラムを記憶する第2の記憶手段とを有する情報処理装置において、前記第1の記憶手段は、複数に分割されたプログラムを実行前に常駐させてあり、前記第2の記憶手段は、分割されたプログラムを実行プログラムとして呼び出す呼び出しプログラムを記憶してあり、前記第2の記憶手段に記憶された呼び出しプログラムを前記セキュアモジュールへ転送すべくしてあり、前記セキュアモジュールは、前記第2の記憶手段に記憶された呼び出しプログラムを受け取る手段と、受け取った呼び出しプログラムを実行可能な状態へ復帰させる手段と、前記CPUが分割されたプログラムを実行する順序で、対応する実行可能な状態へ復帰された呼び出しプログラムを前記第1の記憶手段に書き込む手段と、前記CPUにより実行された呼び出しプログラムを、実行終了後に前記第1の記憶手段から削除する手段とを備えることを特徴とする。

**【0019】**

第6発明に係る情報処理装置では、暗号化されたプログラムを複数に分割し、分割され



たプログラム単位で実行可能な状態へ復帰させ、すべての分割されたプログラムを第1の記憶手段（例えばメモリ）へ書き込んでおく。そして、プログラム間のリンク手段でもある分割されたプログラムを実行プログラムとして呼び出す呼び出しプログラムを暗号化し、分割されたプログラムを実行する順序で呼び出しプログラムを実行可能な状態へ復帰させ、第1の記憶手段へ書き込む。実行が完了した呼び出しプログラムは、第1の記憶手段上から削除する。これにより、プログラム実行時に分割されたプログラムは第1の記憶手段上に書き込まれているが、分割されたプログラム間の関係が不明であることから、悪意ある第三者が第1の記憶手段の内容のイメージコピーを不正に取得した場合であっても、分割されたプログラムの実行順序、実行タイミング等を解析することが困難であり、実行するプログラムの安全性を確保することが可能となる。

#### 【0020】

また、第7発明に係る情報処理装置は、第6発明において、前記第1の記憶手段は、分割されたプログラム間の呼び出し関係を指定する情報であるリンク情報をさらに記憶しており、前記セキュアモジュールは、前記リンク情報に基づいて分割されたプログラムを実行する順序を検出すべくしてあることを特徴とする。

#### 【0021】

第7発明に係る情報処理装置では、分割されたプログラム間の呼び出し関係を指定する情報であるリンク情報に基づいて分割されたプログラムを実行する順序を特定することができ、プログラムの実行順序に従って対応する呼び出しプログラムを実行可能な状態へ復帰させ、第1の記憶手段に書き込む。これにより、一の分割されたプログラムが他の分割されたプログラムを呼び出す場合にのみ対応する呼び出しプログラムが実行可能な状態へ復帰され、第1の記憶手段に書き込まれるので、悪意ある第三者が第1の記憶手段の内容のイメージコピーを不正に取得した場合であっても、第1の記憶手段に書き込まれている呼び出しプログラムに関係のない分割されたプログラムの実行順序、実行タイミング等を解析することは困難であり、実行するプログラム全体の安全性を確保することが可能となる。

#### 【発明の効果】

#### 【0022】

第1発明によれば、プログラム実行時にプログラムのすべての内容が第1の記憶手段上に書き込まれていることがなく、実行時には部分的なプログラムのみが第1の記憶手段へ書き込まれていることから、悪意ある第三者が第1の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム全体の内容を取得することができないことからプログラム内容を解析することができず、実行するプログラムの安全性を確保することが可能となる。

#### 【0023】

また、第2発明によれば、実行要求が出された時点で初めて第1の記憶手段へプログラムが記憶されることから、実行要求が出されるまではプログラムの一部は第1の記憶手段へ書き込まれておらず、外部から第1の記憶手段の内容を参照した場合であってもプログラム全体の内容を把握することは困難であり、実行するプログラムの安全性をより高めることが可能となる。

#### 【0024】

また、第3発明によれば、重要性、秘匿性等の低いプログラムは第1の記憶手段上に常時書き込んでおき、重要性、秘匿性等の高いプログラムは実行時のみ第1の記憶手段に書き込むことで、必要なプログラムのみ実行の安全性を高めることができ、安全性を確保するための処理によるプログラムのオーバーヘッドを低減することが可能となる。

#### 【0025】

また、第4発明によれば、プログラム実行時にプログラムのすべての内容が第1の記憶手段上に書き込まれていることがなく、実行時には部分的なプログラムのみが第1の記憶手段へ書き込まれていることから、悪意ある第三者が第1の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム全体の内容を取得することができない

ことからプログラム内容を解析することができず、実行するプログラムの安全性を確保することが可能となる。

#### 【0026】

また、第5発明によれば、記憶されているプログラムの分割に関する情報に基づいて適正にプログラムを分割することができ、例えば分割単位が不適切であることにより、多くの分割されたプログラムが第1の記憶手段に書き込まれる状態が生じることを回避し、悪意ある第三者が第1の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム内容の解析をより困難にすることができ、実行するプログラムの安全性を確保することが可能となる。

#### 【0027】

また、第6発明によれば、プログラム実行時に分割されたプログラムは第1の記憶手段上に書き込まれているが、分割されたプログラム間の関係が不明であることから、悪意ある第三者が第1の記憶手段の内容のイメージコピーを不正に取得した場合であっても、分割されたプログラムの実行順序、実行タイミング等を解析することが困難であり、実行するプログラムの安全性を確保することが可能となる。

#### 【0028】

また、第7発明によれば、一の分割されたプログラムが他の分割されたプログラムを呼び出す場合にのみ対応する呼び出しプログラムが実行可能な状態へ復帰され、第1の記憶手段に書き込まれるので、悪意ある第三者が第1の記憶手段の内容のイメージコピーを不正に取得した場合であっても、第1の記憶手段に書き込まれている呼び出しプログラムに関係のない分割されたプログラムの実行順序、実行タイミング等を解析することは困難であり、実行するプログラム全体の安全性を確保することが可能となる。

#### 【発明を実施するための最良の形態】

#### 【0029】

以下、本発明をその実施の形態を示す図面に基づいて具体的に説明する。

#### 【0030】

##### (実施の形態1)

以下、本発明の実施の形態1に係る情報処理装置について図面に基づいて具体的に説明する。本実施の形態1では、情報処理装置として一つのコンピュータ、例えばPCを用いて具現化する場合について説明する。もちろん、実行されるプログラムで使用されるデータは、通信手段を介して接続された他のPC、又はDVD等の可搬型記録媒体に記録されていてもよく、通信手段についても特に限定されるものではない。

#### 【0031】

図1は、本発明の実施の形態1に係る情報処理装置の概略構成図である。図1に示すように、情報処理装置1は、少なくとも、CPU(中央演算装置)11、ROM12、RAM(第1の記憶手段)13、記憶手段(第2の記憶手段)14、外部の通信手段と接続する通信インタフェース15、マウス、キーボード等の入力手段と接続する入力インタフェース16、LCD、モニタ、スピーカ等の出力手段と接続する出力インタフェース17、及びセキュアモジュール20と接続するセキュアインタフェース18で構成される。

#### 【0032】

記憶手段14は、ハードディスクに代表される固定型記録媒体、又はDVD、CD-ROM等の可搬型記録媒体であり、実行するプログラム、実行するプログラムで使用されるデータ等を記録する第2の記憶手段である。なお、第2の記憶手段としては、記憶手段14に限定されるものではなく、例えば実行するプログラム、実行するプログラムで使用されるデータ等を記憶するROM12であってもよい。

#### 【0033】

情報処理装置1は、取り外し可能なセキュアモジュール20を着脱可能なセキュアインタフェース18を有する。セキュアインタフェース18は、例えばPCIバスを介してセキュアモジュール20を接続する。セキュアモジュール20は、例えばPCカードによって構成され、DMA(Direct Memory Access)により、CPU11と独立してRAM13

へアクセスすることが可能である。セキュアモジュール 20 は、TRM (Tamper Resistant Module) 構造を有しており、外部から第三者による内容の閲覧を防止することができるとともに、内部データの改竄を防止することができるようになっている。

#### 【0034】

図 2 は、セキュアモジュール 20 の構成の例示図である。図 2 に示すように、セキュアモジュール 20 は、プロセッサ 21、メモリ 22、情報処理装置 1 のセキュアインタフェース 18 を介して通信する通信手段 23 を含む LSI を備える。メモリ 22 は、外部から参照できない不揮発性のフラッシュメモリ (EEPROM) であり、プログラムの難読化情報、暗号化鍵、復号化鍵等の第三者に対して秘匿する必要がある情報が記録されている。

#### 【0035】

情報処理装置 1 は、セキュアモジュール 20 を用いて、プログラムを RAM 13 に書き込んで実行する。記憶手段 14 は、セキュアモジュール 20 のメモリ 22 に記憶している暗号化情報、例えば暗号化鍵によって暗号化されたプログラムを記憶している。また、セキュアモジュール 20 へ暗号化されたプログラムを転送することで、メモリ 22 に記憶している暗号化鍵を用いて該プログラムを復号化することができる。なお、暗号化鍵単独で暗号化／復号化を行うものに限定されるものではなく、暗号化鍵と復号化鍵とを独立して記憶しているものであってもよい。

#### 【0036】

記憶手段 14 に記憶されているプログラムを実行する場合、まず記憶手段 14 に記憶されている暗号化されたプログラムをセキュアモジュール 20 へ転送する。セキュアモジュール 20 は、転送されたプログラムをメモリ 22 に記憶している暗号化鍵を使用して復号するとともに、プログラムの命令コードを解析して、複数のプログラム部品へ分割する。図 3 は、プログラム分割の例示図である。図 3 に示すように、分割されたプログラム部品は、プログラム 40 の一部を構成するプログラムコードである。プログラム 40 が動作するときには、例えばプログラム部品 41～43 が互いに他のプログラム部品 41～43 を呼び出す、又は他のプログラム部品 41～43 へジャンプしながら、1つのプログラム 40 として動作する。プログラム部品は、最小単位としてプロセッサの命令 1 つから構成される。

#### 【0037】

なお、プログラムの分割については、本実施の形態 1 のように、セキュアモジュール 20 がプログラムを解析してプログラム部品に分割してもよいが、斯かる方法に限定されるものではなく、事前に、プログラム分割に関する情報、例えば分割単位に関する情報を付加して該プログラムを記憶手段 14 に記憶しておき、セキュアモジュール 20 での復号時に、斯かる情報に基づいて分割する方法であってもよい。プログラム分割に関する情報に基づいてプログラムを分割することで、プログラムを適切に分割することができ、例えば分割単位が不適切であることにより、多くの分割されたプログラムが実行可能な状態で RAM 13 に書き込まれている状態が生じることを回避し、悪意ある第三者が RAM 13 の内容のイメージコピーを不正に取得した場合であっても、プログラム内容の解析をより困難にすることができ、実行するプログラムの安全性を確保することが可能となる。

#### 【0038】

また、記憶手段 14 に暗号化されたプログラムとして記憶する時点で、複数のプログラム部品として記憶するものであってもよい。この場合、セキュアモジュール 20 は、転送されたプログラム部品を、メモリ 22 に記憶している暗号化鍵を使用して復号する。

#### 【0039】

次に、セキュアモジュール 20 は、最初に動作する部分であるプログラム部品、例えばプログラム部品 41 を RAM 13 へ書き込む。RAM 13 へ書き込まれた後、CPU 11 は、書き込まれたプログラム部品 41 を実行する。プログラム部品 41 を実行し、他のプログラム部品の実行を要求する命令コードが存在する場合、該命令コードを実行するタイミングで、セキュアモジュール 20 は要求される他のプログラム部品、例えばプログラム

部品 42、43 を RAM 13 へ書き込む。CPU 11 は、RAM 13 への書き込み完了通知を受け取った後、書き込まれたプログラム部品 42、43 を順次実行する。

#### 【0040】

書き込まれたプログラム部品の実行が完了した場合、RAM 13 へ書き込まれたプログラム部品は、CPU 11 が RAM 13 から消去する。したがって、プログラム全体が RAM 13 へ書き込まれていることがなく、プログラムを構成するプログラム部品の一部のみが RAM 13 へ書き込まれながら、プログラムが実行される。

#### 【0041】

このように、プログラム全体を RAM 13 へ書き込まないことから、悪意ある第三者により RAM 13 のイメージコピーを不正に取得された場合であっても、イメージコピーには、プログラム全体のうちの一部のプログラム部品しか書き込まれておらず、逆解析によりプログラムの全容を把握することが困難であり、実行するプログラムの安全性を確保することが可能となる。

#### 【0042】

ここで、セキュアモジュール 20 は、CPU 11 と独立して動作する。したがって、RAM 13 へ書き込まれたプログラムが、他のプログラム部品を必要とするタイミングをセキュアモジュール 20 へ通知する必要がある。CPU 11 が、セキュアモジュール 20 へ他のプログラム部品を必要とするタイミングを通知する手段としては種々の方法が用いられる。例えば、実行するプログラムが、セキュアモジュール 20 との間で実行タイミングの同期を取ることが可能な構造を有するプログラムである場合、該プログラムが要求するプログラム部品が実行される直前に、セキュアモジュール 20 により対応するプログラム部品を RAM 13 へ書き込む方法を用いる。

#### 【0043】

図 4 は、実行するプログラムが要求するプログラム部品が実行される直前に、セキュアモジュール 20 により対応するプログラム部品を RAM 13 へ書き込む方法の説明図である。図 4 (a) に示すように、プログラムの中に条件分岐命令を設定する。該条件分岐命令の条件は一定値とし、必ず一方の経路を選択するようにしておく。他方の経路には無効なプログラム部品を配置する。無効なプログラム部品は、例えば nop 列、0 列等、動作しないプログラムコードである。なお、無効なプログラム部品が配置された領域に、要求されたプログラム部品の書き込み可能領域を確保しておく。

#### 【0044】

セキュアモジュール 20 は、RAM 13 へ書き込まれていないプログラム部品の実行が必要になったタイミング、すなわちプログラム部品の実行要求命令がプログラムで実行された時点で、図 4 (b) に示すように、RAM 13 の無効なプログラム部品が配置された領域のプログラム部品の書き込み可能領域に、要求されたプログラム部品を書き込む。なお、RAM 13 へ該プログラム部品が書き込まれた後、図 4 (c) に示すように該プログラム部品を要求したプログラムの条件分岐命令の条件を変更し、他方の経路を選択するようにして、CPU 11 が、書き込まれたプログラム部品を実行する。

#### 【0045】

実行されるプログラムが、セキュアモジュール 20 との間で実行タイミングの同期を取ることが可能な構造を有さないプログラムである場合、セキュアモジュール 20 は、プログラムを RAM 13 へ書き込む時点で、プログラム部品の実行を要求する実行要求プログラムを該プログラムへ挿入する。セキュアモジュール 20 は、挿入した実行要求プログラムの実行に応じて、対応するプログラム部品を RAM 13 へ書き込む。

#### 【0046】

プログラムのうち、どのプログラム部品を常に RAM 13 へ書き込み、どのプログラム部品をいつ RAM 13 へ書き込むべきかについては、事前にセキュアモジュール 20 に書込情報として記憶しておく。これにより、重要な秘密情報を扱うプログラム部品が RAM 13 に常駐することを回避することができ、より安全性を高めることができる。書込情報としては、「常に RAM 13 へ書き込み」、「実行時に RAM 13 へ書き込み」、「セキ

ュアモジュールが選択」の3種類がある。

#### 【0047】

図5は、プログラム部品を動的にRAM13へ書き込む場合の説明図である。図5(a)に示すように、プログラムの実行開始時には、プログラム部品41をRAM13へ書き込む。プログラム部品42はRAM13へ書き込まず、セキュアモジュール20に対してプログラム部品42の実行要求を行う実行要求プログラム50をRAM13へ書き込む。実行要求プログラム50は、セキュアモジュール20で生成してもよいし、あらかじめセキュアモジュール20に記録しておいてもよい。プログラム部品41は、プログラム部品42を呼び出すプログラムではなく、実行要求プログラム50を呼び出す。

#### 【0048】

プログラムが実行されると、プログラム部品41は、最後に実行要求プログラム50を呼び出す。実行要求プログラム50が実行されると、図5(b)に示すように、セキュアモジュール20は、要求されたプログラム部品42をRAM13へ書き込む。セキュアモジュール20によりプログラム部品42がRAM13へ書き込まれた後、CPU11がプログラム部品42を実行することにより、プログラム部品42をプログラム部品41から直接呼び出した場合と同様に実行することができる。

#### 【0049】

セキュアモジュール20は、プログラム部品42のRAM13への書き込みの完了を検知するため、実行要求プログラム50の末尾に、例外処理を生じる命令を設定しておく。CPU11が、実行要求プログラム50を実行し、末尾に設定された例外処理を生じる命令を実行した場合、CPU11は、プログラムの実行を一旦停止させ、セキュアモジュール20に対してRAM13への書き込み完了通知を送信する。これにより、セキュアモジュール20は、割り込み命令、アクセス違反等の例外処理を生じる命令を実行要求プログラム50に付加し、実行要求プログラム50を実行するだけであることから、例えばプログラムの待機を行うプログラムを直接呼び出す場合のように、待機処理を行っているプログラムを特定することが困難になる。したがって、第三者にとってはより解析しにくい形でプログラム部品のRAM13への書き込みの完了を待つことが可能となる。

#### 【0050】

以上のように本実施の形態1によれば、セキュアモジュール20がプログラムを複数のプログラム部品に分割し、分割されたプログラム部品単位でRAM13へ書き込み、実行することから、悪意ある第三者にRAM13のイメージコピーを取得された場合であっても、プログラムの全体像を把握することが困難であり、プログラムの安全性を確保することが可能となる。

#### 【0051】

##### (実施の形態2)

実施の形態2に係る情報処理装置1は、実施の形態1と同様の構成であるが、実施の形態1のようにプログラム部品自体をセキュアモジュール20から動的にRAM13へ書き込むのではなく、プログラム部品はRAM13へ常時書き込んでおき、各プログラム部品中の他のプログラム部品の呼び出しアドレスだけを更新する。図6は、本実施の形態2に係る情報処理装置でのプログラム部品実行方法の説明図である。

#### 【0052】

図6(a)に示すように、最初のプログラムをRAM13へ書き込んだ時点では、プログラム部品41からプログラム部品42、43を呼び出す部分には無効なアドレスを記録しておく。したがって、イメージコピーを取得した第三者が解析しても、プログラム部品41がどのプログラム部品をプログラム実行中に呼び出すのか不明となる。そして、図6(b)に示すように、プログラム部品41からプログラム部品42、43を呼び出すタイミングで、セキュアモジュール20は、プログラム部品41の中の呼び出しアドレスを、次に実行するプログラム部品が存在するアドレスへ書き換える。この結果、プログラム部品41からプログラム部品42が呼び出され、プログラム部品42を実行することができる。

**【0053】**

以上のように本実施の形態2によれば、実施の形態1のようにプログラム部品自体をRAM13へ書き込むのではなく、呼び出しアドレスの書き換えのみを行えばよいことから、プログラム部品をRAM13へ書き込む時間に比べて短時間でアドレス書き換えを行うことができ、全体の処理時間を短縮することが可能となる。

**【0054】**

なお、実施の形態1及び2を組み合わせることにより、呼び出し元プログラム部品の呼び出し先アドレスの書き換えと、プログラム部品のRAM13への書き込みを同時に行い、プログラム部品が動的にRAM13へ書き込まれ、かつRAM13へ書き込まれるごとに呼び出しアドレスが変化するようにしてもよい。これにより、より実行するプログラムの安全性を高めることが可能となる。

**【0055】**

(実施の形態3)

以下、実行するプログラムを事前に分割してRAM13へ書き込む場合の実施例について説明する。図7は、本発明の実施の形態3に係る情報処理装置1で実行するプログラムのプログラム部品への分割の説明図である。図7に示すように、実行するプログラム40を、あらかじめプログラム部品41～43に分割しておき、分割されたプログラム部品41～43に対して、それぞれ書込情報410～430、特殊コード情報411～431、部品リンク情報412～432からなる付加情報を記憶する。書込情報410～430は、プログラム部品41～43をRAM13へどのタイミングで書き込むのかを示す情報である。特殊コード情報411～431は、プログラム部品41～43が特殊コードであるか否か、及びどのような特殊コードであるのかを示す情報である。部品リンク情報412～432は、プログラム部品同士がどのように呼び出されるかを記述する情報である。

**【0056】**

図8は、書込情報410、特殊コード情報411、及び部品リンク情報412の例示図である。プログラム部品41は、CPU11が実行可能なプログラムコードである。書込情報410は、「常にメモリに書き込む」という情報を記憶している。特殊コード情報411は、「オフセット50hのアドレスから秘密データを渡す特殊コードである」という情報を記憶している。部品リンク情報412は、「オフセット100hのアドレスからプログラム部品42のオフセットアドレス10hを呼び出す」、及び「アドレス320hからプログラム部品43のオフセットアドレス30hを呼び出す」という情報を記憶している。

**【0057】**

なお、部品リンク情報は複数の情報を含んでもよい。また、特殊コード情報も複数の特殊コード情報を含んでもよい。これらプログラム部品に関する情報は、セキュアモジュール20の外部から参照することができないメモリ22に記憶されている暗号化鍵で暗号化され、セキュア化プログラムデータ30として記憶手段14に記憶される。

**【0058】**

図9は、プログラムの実行開始時の動作の説明図である。プログラムを実行する場合、まず基本プログラム60が動作する。基本プログラム60は、記憶手段14からセキュア化プログラムデータ30を読み出す。次に、基本プログラム60は、プログラム40が動作するための実行領域100をRAM13に確保する。そしてセキュア化プログラムデータ30と、プログラム実行用に確保した実行領域100のアドレスをセキュアモジュール20に渡す。

**【0059】**

セキュアモジュール20は、セキュア化プログラムデータ30を外部から参照することができないメモリ22に記憶されている暗号化鍵を用いて復号する。そして、実行すべきプログラム部品41をRAM13の実行領域100へ書き込む。CPU11は、基本プログラム60にて実行領域100へ書き込まれたプログラム部品41の開始アドレスが呼び出された場合、プログラム部品41の実行を開始する。

**【0060】**

図 1.0 は、プログラムの実行開始時のセキュアモジュール 2 0 での処理のフローチャートである。図 1 0 に示すように、セキュアモジュール 2 0 は、セキュア化プログラムデータ 3 0 を外部から参照することができないメモリ 2 2 に記憶されている暗号鍵を用いて復号する（ステップ S 1 0 0 1）。セキュア化プログラムデータ 3 0 を復号した後、各プログラム部品に付加されている書込情報の内容を確認する（ステップ S 1 0 0 2）。書込情報に R A M 1 3 へ書き込む旨が記憶されている場合（ステップ S 1 0 0 3：Y E S）、記憶されているプログラム部品を R A M 1 3 の実行領域 1 0 0 へ書き込む（ステップ S 1 0 0 4）。

#### 【0 0 6 1】

次に、セキュアモジュール 2 0 は、プログラム部品の特殊コード情報の有無を確認する（ステップ S 1 0 0 5）。特殊コード情報が有る場合（ステップ S 1 0 0 6：Y E S）、特殊コードに従った呼び出し処理を実行する（ステップ S 1 0 0 7）。特殊コード呼び出し処理の詳細については後述する。すべてのプログラム部品について上述した処理を繰り返す（ステップ S 1 0 0 8）。

#### 【0 0 6 2】

すべてのプログラム部品につき上述した処理が完了した場合（ステップ S 1 0 0 8：Y E S）、プログラム部品間のリンク処理を実行する（ステップ S 1 0 0 9）。プログラム部品間のリンク処理の詳細についても後述する。リンク処理が完了した時点でプログラムの実行準備が完了する。プログラムの実行準備が完了した旨は、割り込み処理、状態レジスタ等により情報処理装置（P C）1 に通知する。

#### 【0 0 6 3】

セキュアモジュール 2 0 が行う特殊コード呼び出し処理は、セキュアモジュール 2 0 が動作タイミングを制御する部分のプログラムコード呼び出し処理である。図 1 1 及び図 1 2 は、セキュアモジュール 2 0 が行う特殊コード呼び出し処理の説明図である。図 1 1 は、特殊コード情報、リンク情報等の例示図である。図 1 1 の例では、プログラム部品 4 1 には、「オフセット 50h のアドレスからプログラム部品 4 5 を呼び出す」という部品リンク情報 4 1 2 が付加されている。また、プログラム部品 4 5 は、「コンテンツ鍵変更時に実行」という特殊コード情報 4 5 1 を含んでいる。

#### 【0 0 6 4】

セキュアモジュール 2 0 は、特殊コード呼び出し部 8 0 を R A M 1 3 へ書き込み、特殊コード呼び出し部 8 0 をプログラム部品 4 1 から呼び出すようリンクする。特殊コード呼び出し部 8 0 は、セキュアモジュール 2 0 で自動生成してもよいし、プログラム部品としてセキュア化プログラムデータ 3 0 に含めておいてもよい。

#### 【0 0 6 5】

R A M 1 3 へ書き込んだ特殊コード呼び出し部 8 0 は、条件分岐から参照されるデータ、条件分岐コード及び特殊コードを呼び出す部分からなる。図 1 2（a）には、特殊コード呼び出し部 8 0 がアドレス 13845fa0h に書き込まれる例が示されている。その先頭には条件分岐で参照されるデータが埋め込まれている。

#### 【0 0 6 6】

通常、先頭に埋め込まれる条件分岐で参照される値は 0 である。特殊コードの実行条件を具備しない間は 0 のままである。図 1 2（a）の条件分岐では、アドレス 13845fa0h に記憶された値が 0 である場合、即座にリターンするようにしておく。これにより、プログラム部品 4 1 から特殊コード呼び出し部 8 0 が呼び出された場合であっても、特殊コードの実行条件を具備しない場合は即座にリターンすることができる。

#### 【0 0 6 7】

条件分岐で参照される値が 0 でない場合は、続くプログラムコードが実行される。続くプログラムコードは、分岐条件で参照される値に 0 を設定するコードと、プログラムの実行領域 1 0 0 を呼び出すコードから構成される。プログラム実行開始時の初期書き込み時には、プログラムの実行領域 1 0 0 には無効なプログラムデータが書き込まれている。

#### 【0 0 6 8】

プログラムの実行中に、特殊コードの実行条件を具備した場合、セキュアモジュール 20 は、実行領域 100 に、実行条件を具備した特殊コードを書き込む。図 12 (b) の例では、特殊コードは「コンテンツ鍵変更時に実行」されるというコードであることから、セキュアモジュール 20 は、コンテンツ鍵の変更直前に実行領域 100 へプログラム部品 45 を書き込む。プログラム部品 45 を書き込んだ後、アドレス 13845fa0h の条件分岐から参照されるデータを書き換える。書き換えることにより、特殊コードの実行条件を具備した状態となる。特殊コードの実行条件を具備した状態で、特殊コード呼び出し部 80 が実行されると、即座にリターンすることなく、条件分岐で参照される値に 0 を設定するコードと、プログラム部品 45 を呼び出すコードが実行される。

#### 【0069】

次にセキュアモジュール 20 が実行するプログラムリンク処理について述べる。プログラムリンク処理は、任意のプログラム部品を動的に書き込む処理である。図 13 及び図 14 は、プログラム部品の動的書き込み処理及びリンク処理についての説明図である。図 13 は、プログラム部品 41 に関連する書き込み処理及びリンク処理での書込情報、リンク情報等の例示図である。

#### 【0070】

図 13 の例では、プログラム部品 41 に対応する部品リンク情報 412 から、プログラム部品 41 はプログラム部品 42 とプログラム部品 43 の呼び出しを含んでいることがわかる。それぞれの書込情報 420、430 を参照すると、プログラム部品 42 は実行時まで RAM 13 に書き込まず、プログラム部品 43 は開始時に RAM 13 に書き込まれるように記述されている。プログラム部品 43 は常に RAM 13 に書き込まれるコードであることから、プログラム部品 41 の実行開始時に、プログラム部品 41 からプログラム部品 43 の呼び出しは実行される。

#### 【0071】

図 14 (a) では、プログラム部品 43 は、RAM 13 のアドレス 13900000h の領域に書き込まれている。そこで、プログラム部品 41 のオフセット 320h にあるプログラム部品 43 の呼び出しコマンドには、プログラム部品 43 のアドレスを設定する。本実施例では、プログラム部品 43 のオフセット 30h を呼び出しているので、プログラム部品 41 には、13900030h を呼び出すよう呼び出しコマンドの呼び出し先アドレスを設定しておく。

#### 【0072】

一方、プログラム部品 42 は、プログラム部品 41 の実行開始時に RAM 13 に書き込まれていないので、プログラム部品 42 の実行依頼コードを RAM 13 へ書き込んでおき、プログラム部品 41 からは実行依頼コードを呼び出すようにしておく。実行依頼コードは、例えばセキュアモジュール 20 のレジスタアドレスへの書き込みプログラムにより実現される。

#### 【0073】

実行依頼コードの末尾には、例外処理を発生するコードと、キャッシュフラッシュ命令と、プログラム部品 42 本体の呼び出しコードとが含まれる。本実施例では例外処理を発生するコードとして int 3 命令を使用しているが、これ以外の例外処理、例えばメモリアクセス違反を起こすようなコードを使用してもよい。また、プログラム部品 42 の書き込まれるアドレスが一定ではないようにしており、呼び出しアドレスには無効な値を記憶している。さらに、キャッシュフラッシュ命令を用いてキャッシュを一旦クリアし、セキュアモジュール 20 が設定した呼び出しアドレスが確実に呼び出されるようにしている。キャッシュフラッシュ命令はアーキテクチャに依存するものであることから、アーキテクチャによっては使用できない。

#### 【0074】

プログラムの実行が開始される場合、図 14 (b) に示すように、プログラム部品 41 が実行され、プログラム部品 42 の実行依頼コードが実行されると、PC からセキュアモジュール 20 に、プログラム部品 42 の RAM 13 への書き込みが要求される。そして、プログラムは、次の例外処理発生コード (int 3) を実行し、割り込みハンドラが起動される



。割り込みハンドラは、セキュアモジュール 20 からのプログラム書き込み完了割り込み処理が発生するまで待機し、割り込み処理の発生後、続きのコードを実行するようにしておく。実行依頼を受けたセキュアモジュール 20 は、プログラム部品 42 を RAM 13 へ書き込むと共に、呼び出し元の呼び出し先アドレスを設定する。

**【0075】**

本実施例では、アドレス 13A00000h の領域にプログラム部品 42 を書き込むと共に、呼び出し先アドレスを 13A00010h (プログラム部品 42 のオフセット 10h) に設定している。プログラム部品 42 の書き込みは、事前に書き込んでおいてもよいし、プログラム部品 42 の呼び出しアドレスを固定しておいてもよい。

**【0076】**

以上説明したように、本発明ではセキュアモジュールを利用し、プログラムを動的に RAM 上に書き込み又はプログラムの呼び出しアドレスを動的に変更することにより、悪意ある第三者にとって解析が困難な形態でプログラムを実行することが可能となる。

**【図面の簡単な説明】****【0077】**

【図 1】 本発明の実施の形態 1 に係る情報処理装置の概略構成図である。

【図 2】 セキュアモジュールの構成の例示図である。

【図 3】 プログラム分割の例示図である。

【図 4】 プログラム部品を RAM へ記憶する方法の説明図である。

【図 5】 プログラム部品を動的に RAM へ記憶する場合の説明図である。

【図 6】 本実施の形態 2 に係る情報処理装置でのプログラム部品実行方法の説明図である。

【図 7】 本発明の実施の形態 3 に係る情報処理装置で実行するプログラムのプログラム部品への分割の説明図である。

【図 8】 書込情報、特殊コード情報、及び部品リンク情報の例示図である。

【図 9】 プログラムの実行開始時の動作の説明図である。

【図 10】 プログラムの実行開始時のセキュアモジュールでの処理のフローチャートである。

【図 11】 セキュアモジュールが行う特殊コード呼び出し処理の説明図である。

【図 12】 セキュアモジュールが行う特殊コード呼び出し処理の説明図である。

【図 13】 プログラム部品の動的書き込み処理及びリンク処理についての説明図である。

【図 14】 プログラム部品の動的書き込み処理及びリンク処理についての説明図である。

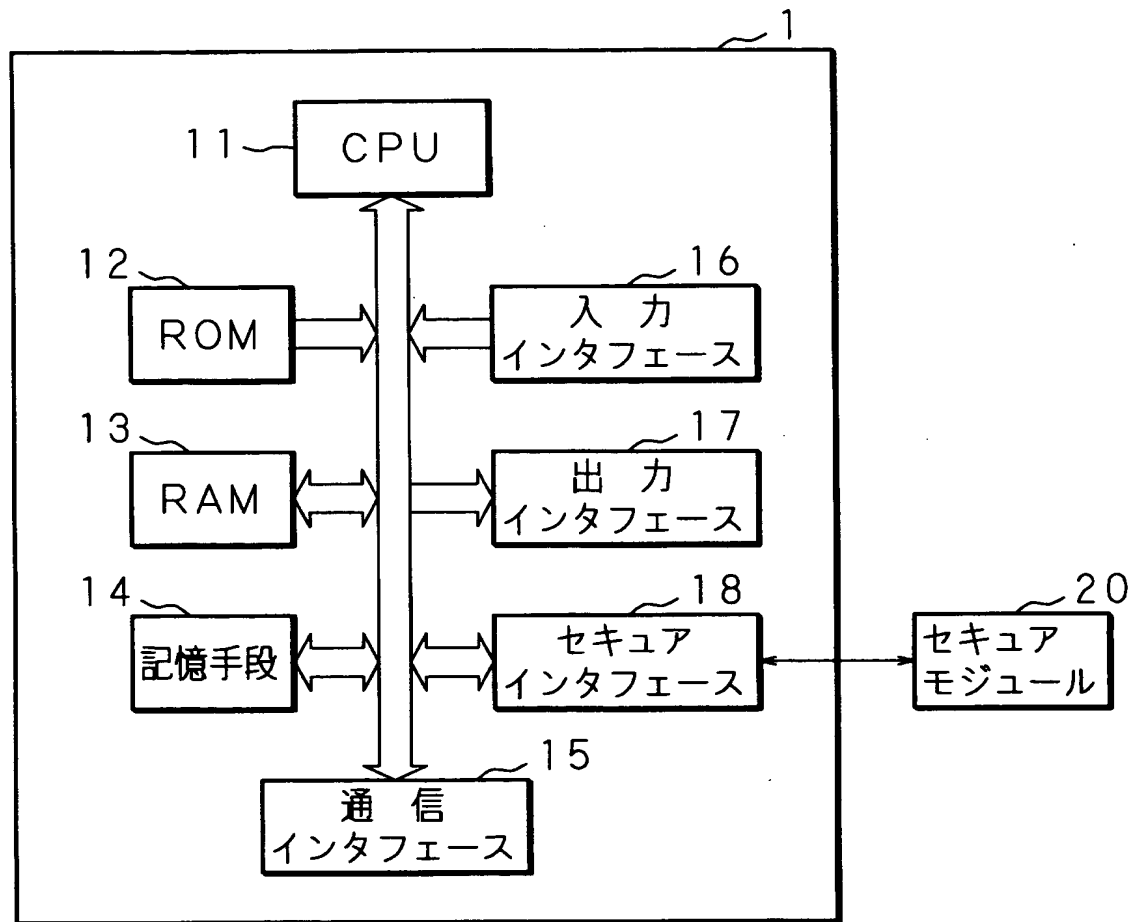
**【符号の説明】****【0078】**

- 11 CPU
- 12 ROM
- 13 RAM (第 1 の記憶手段)
- 14 記憶手段 (第 2 の記憶手段)
- 15 通信インタフェース
- 16 入力インタフェース
- 17 出力インタフェース
- 18 セキュアインタフェース
- 20 セキュアモジュール
- 21 プロセッサ
- 22 メモリ
- 23 通信手段
- 30 プログラムデータ
- 40 プログラム

4 1、4 2、4 3、4 5 プログラム部品  
5 0 実行要求プログラム  
6 0 基本プログラム  
8 0 特殊コード呼び出し部  
1 0 0 実行領域  
4 1 0、4 2 0、4 3 0 書込情報  
4 1 1、4 2 1、4 3 1、4 5 1 特殊コード情報  
4 1 2、4 2 2、4 3 2 部品リンク情報

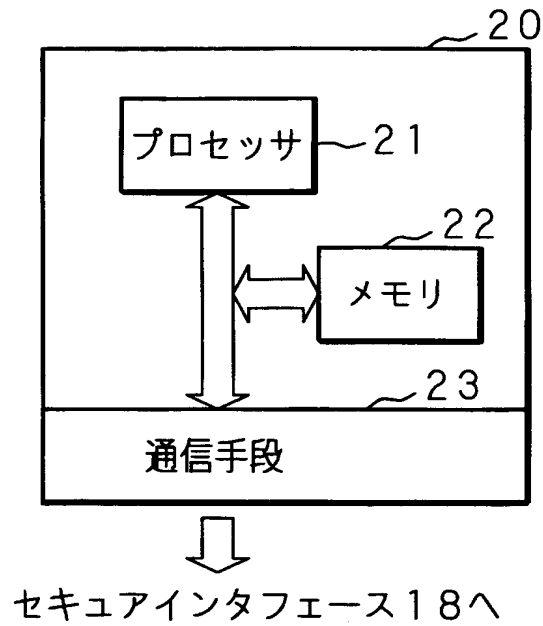
【書類名】 図面  
【図 1】

本発明の実施の形態 1 に係る情報処理装置の概略構成図



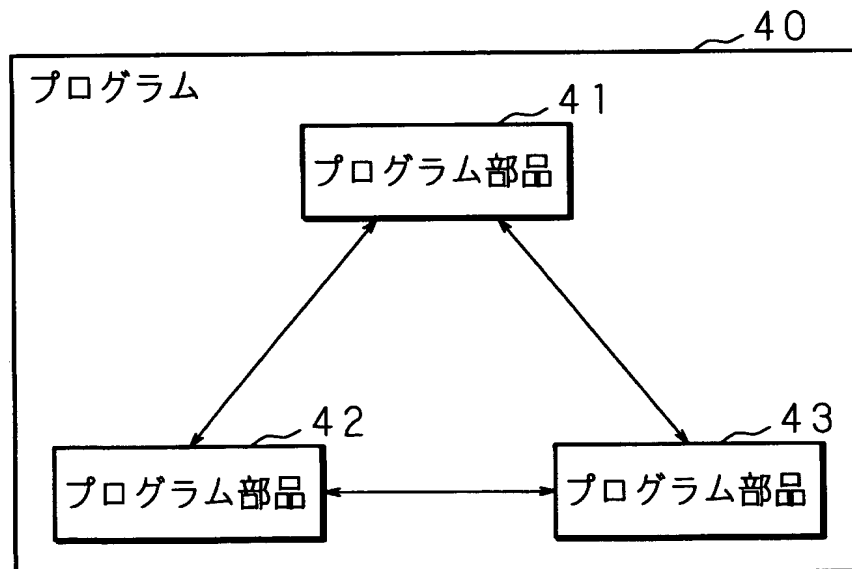
【図 2】

セキュアモジュールの構成の例示図



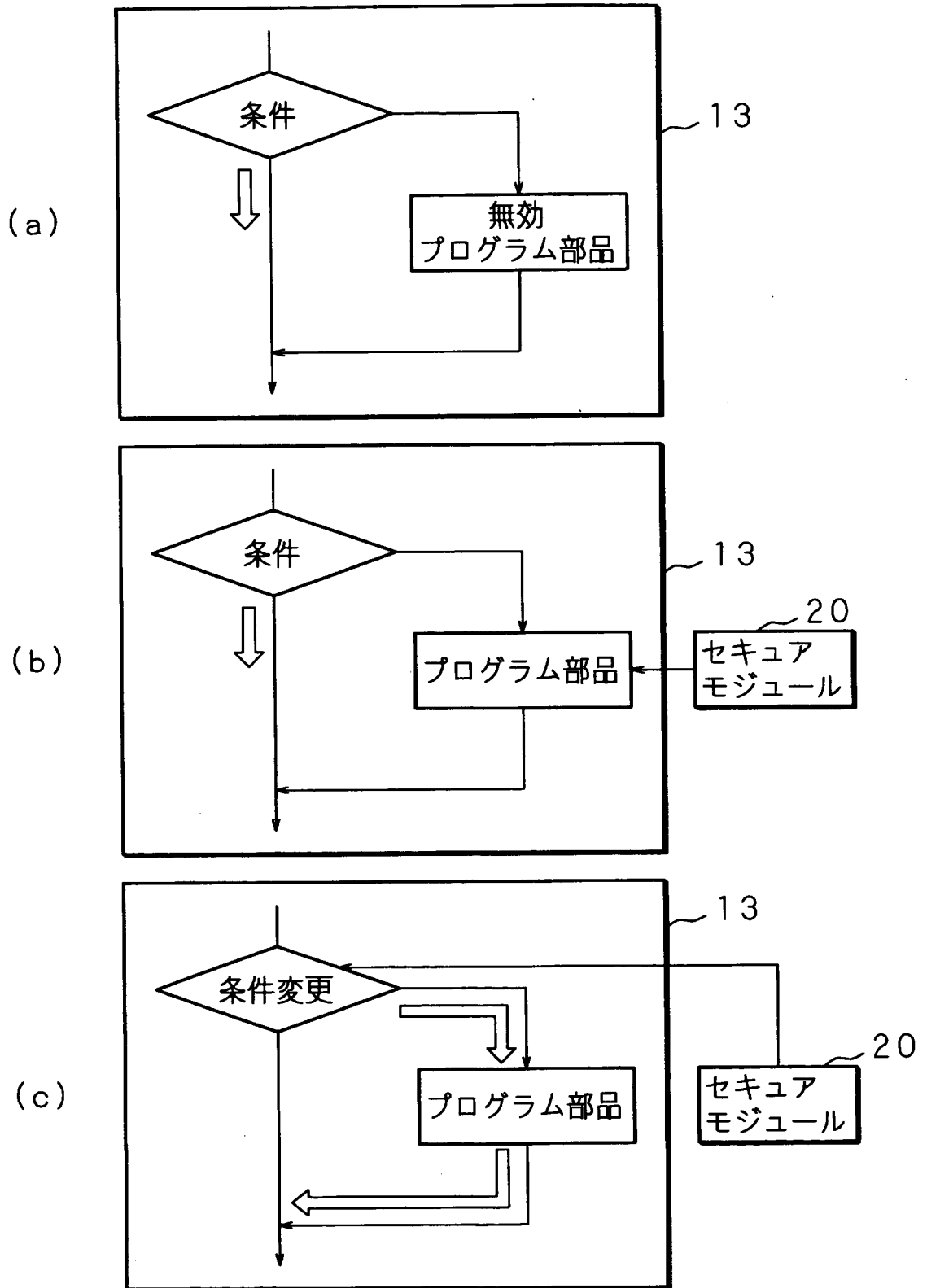
【図 3】

プログラム分割の例示図



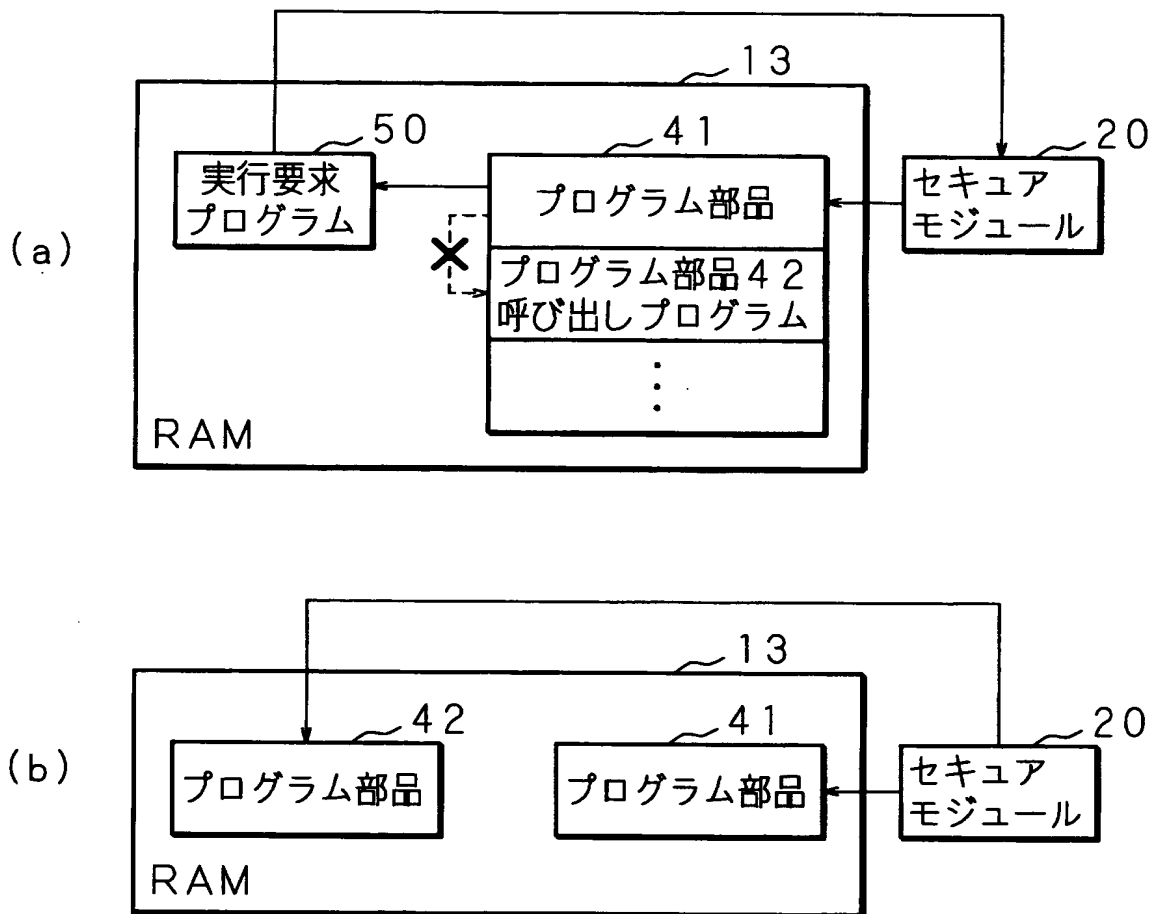
【図4】

## プログラム部品をRAMへ記憶する方法の説明図



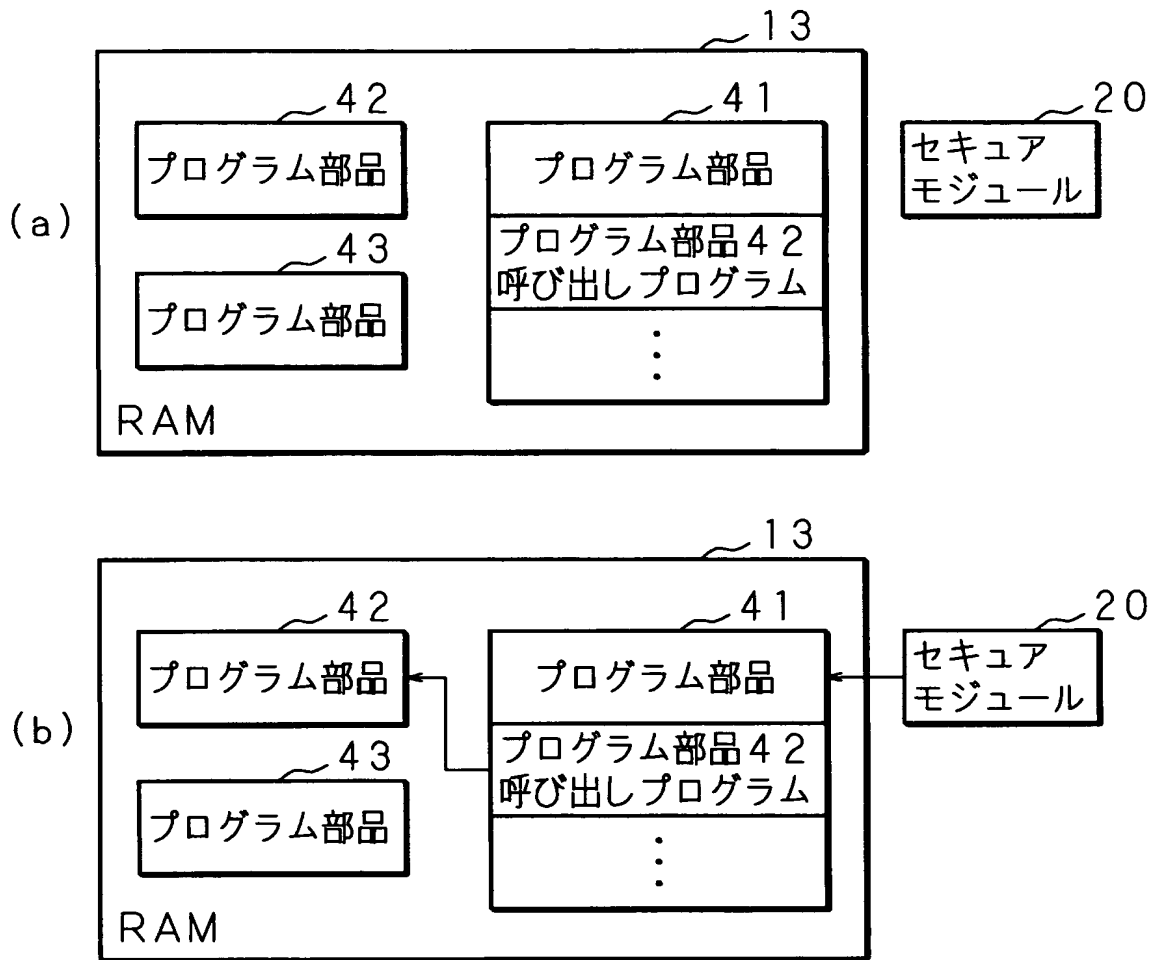
【図 5】

プログラム部品を動的にRAMへ記憶する場合の説明図



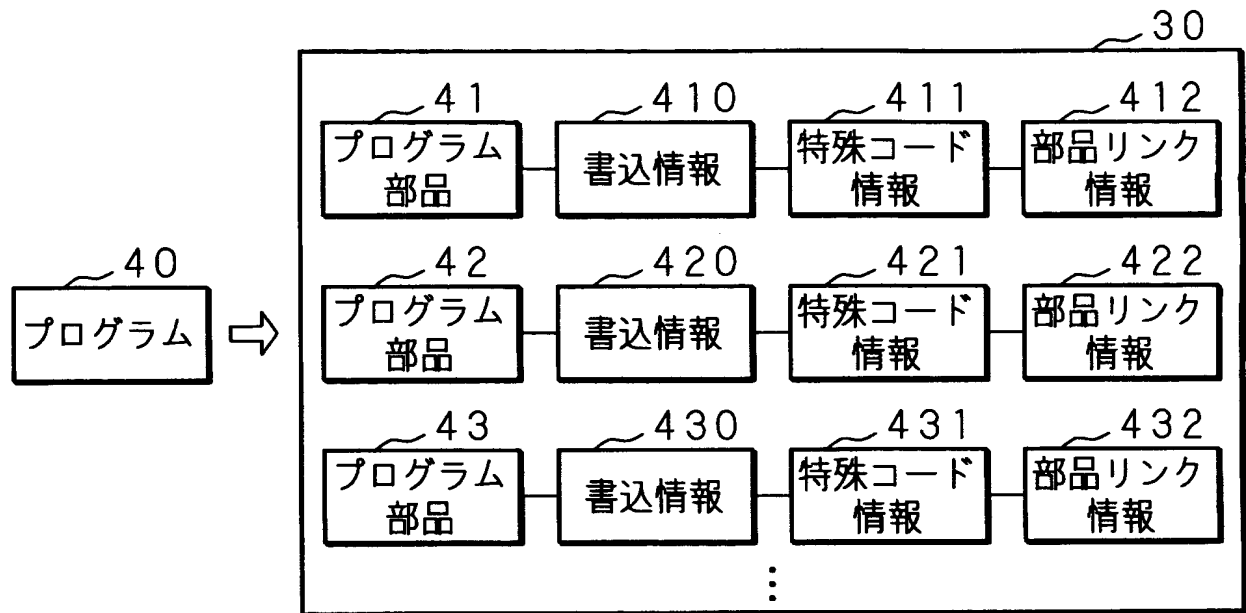
【図 6】

本実施の形態 2 に係る情報処理装置での  
プログラム部品実行方法の説明図



【図 7】

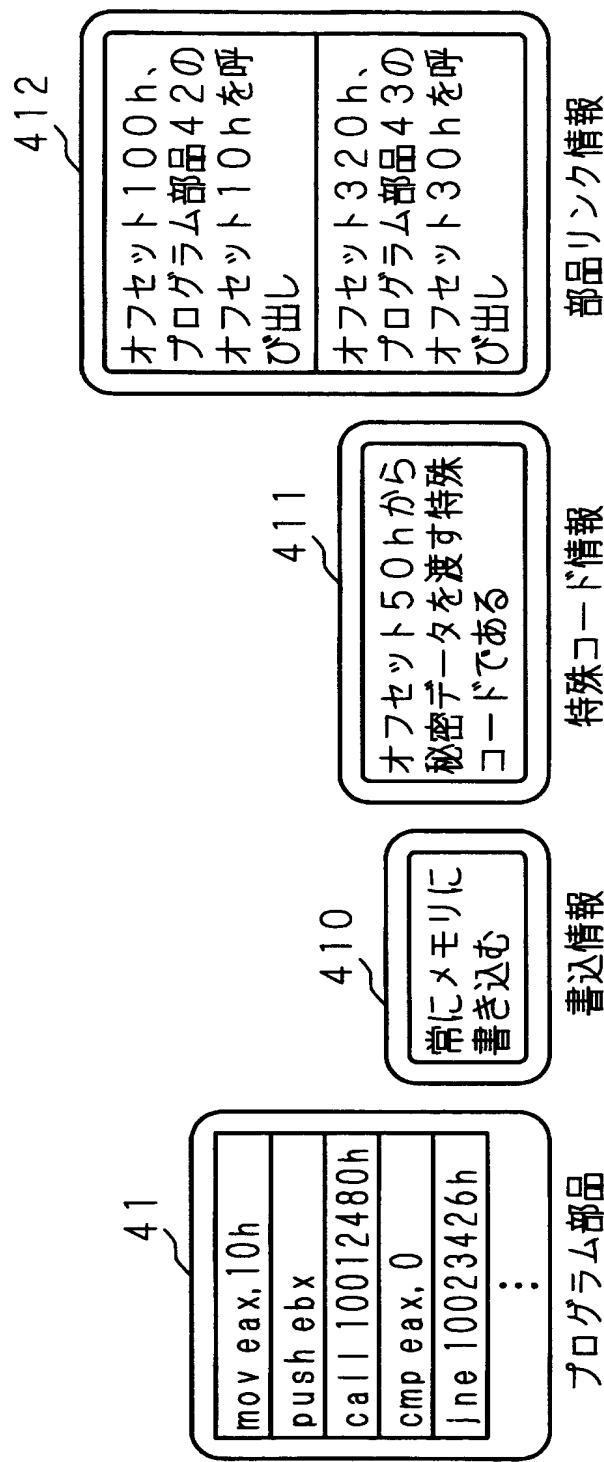
本発明の実施の形態 3 に係る情報処理装置で実行する  
プログラムのプログラム部品への分割の説明図





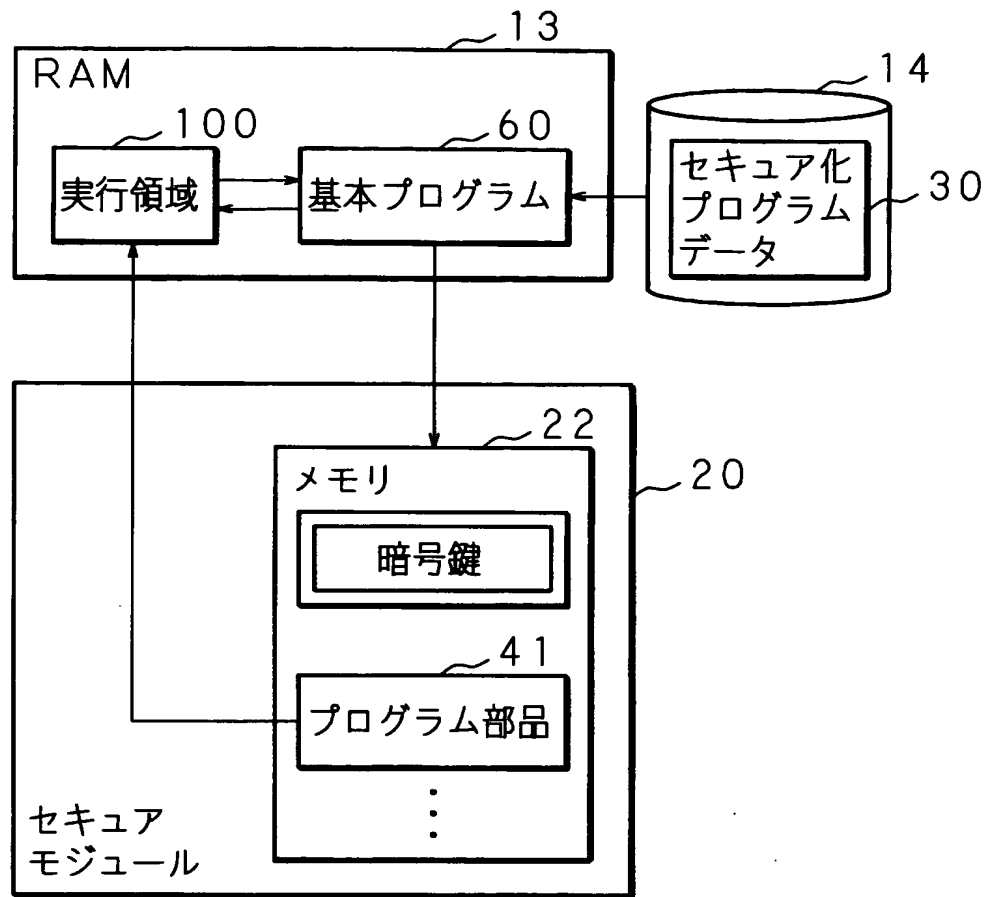
【図 8】

書込情報、特殊コード情報、及び部品リンク情報の例示図



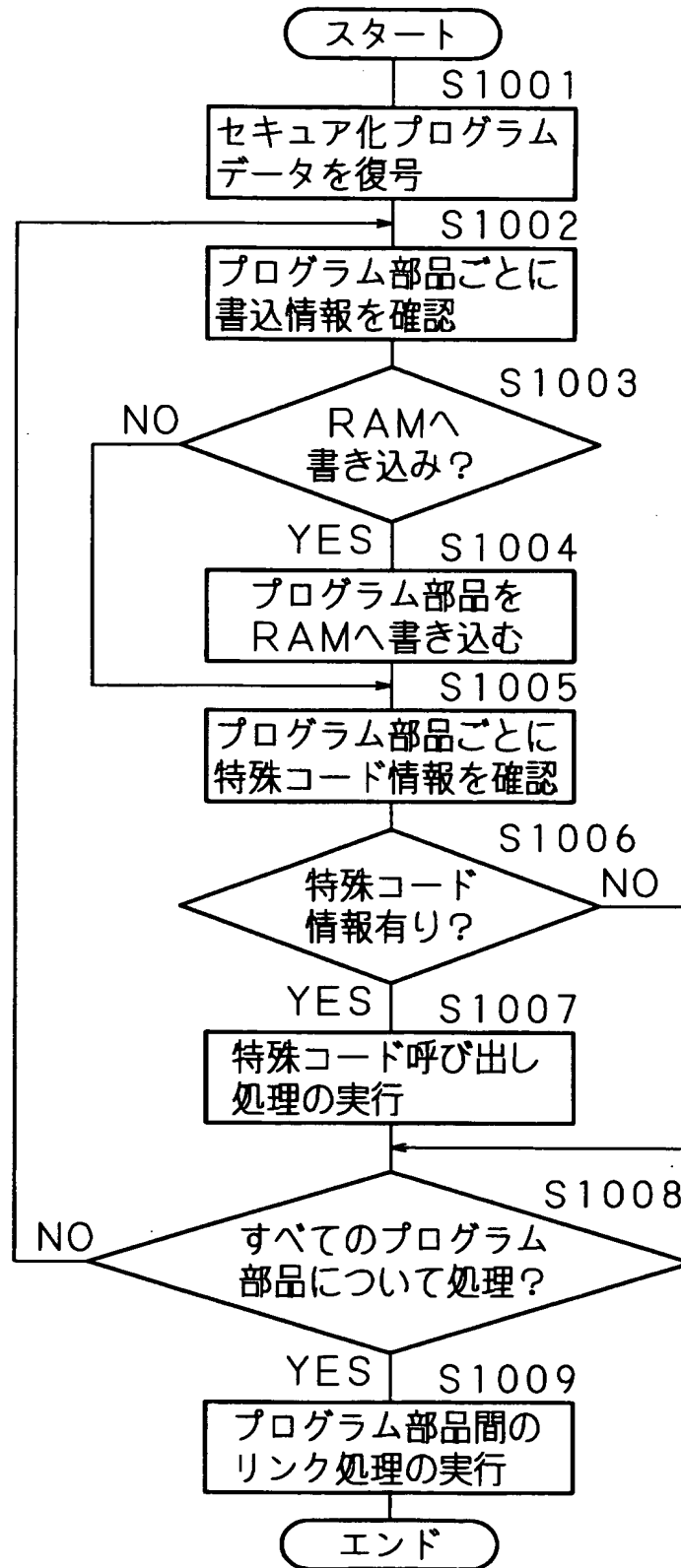
【図 9】

プログラムの実行開始時の動作の説明図



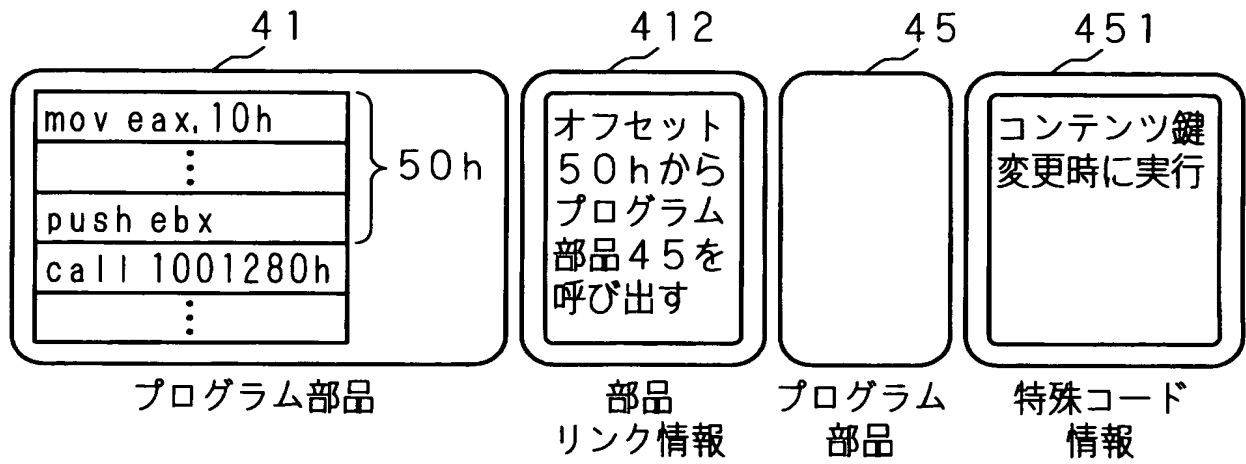
【図 10】

プログラムの実行開始時のセキュアモジュールでの処理のフローチャート



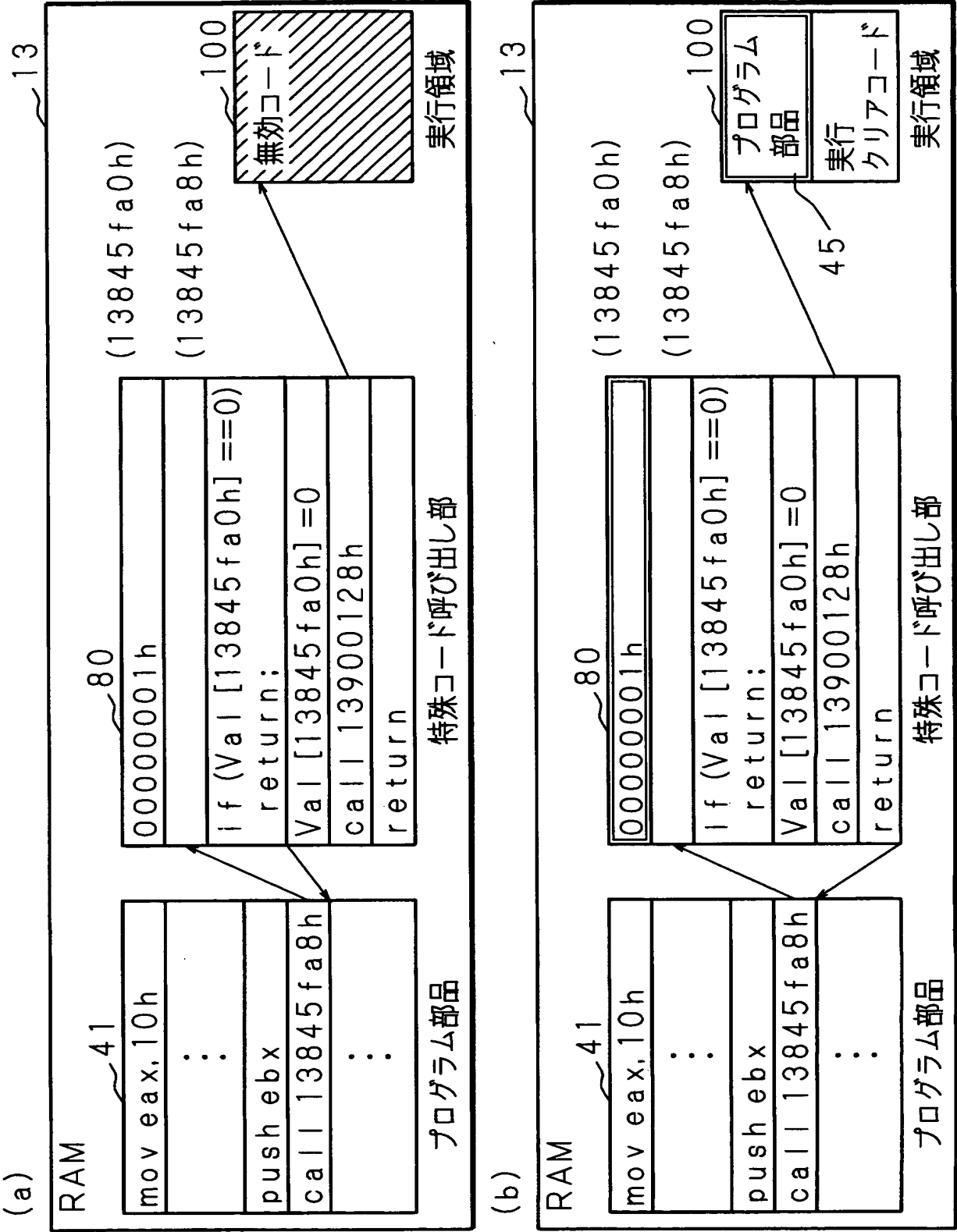
【図 11】

セキュアモジュールが行う特殊コード呼び出し処理の説明図



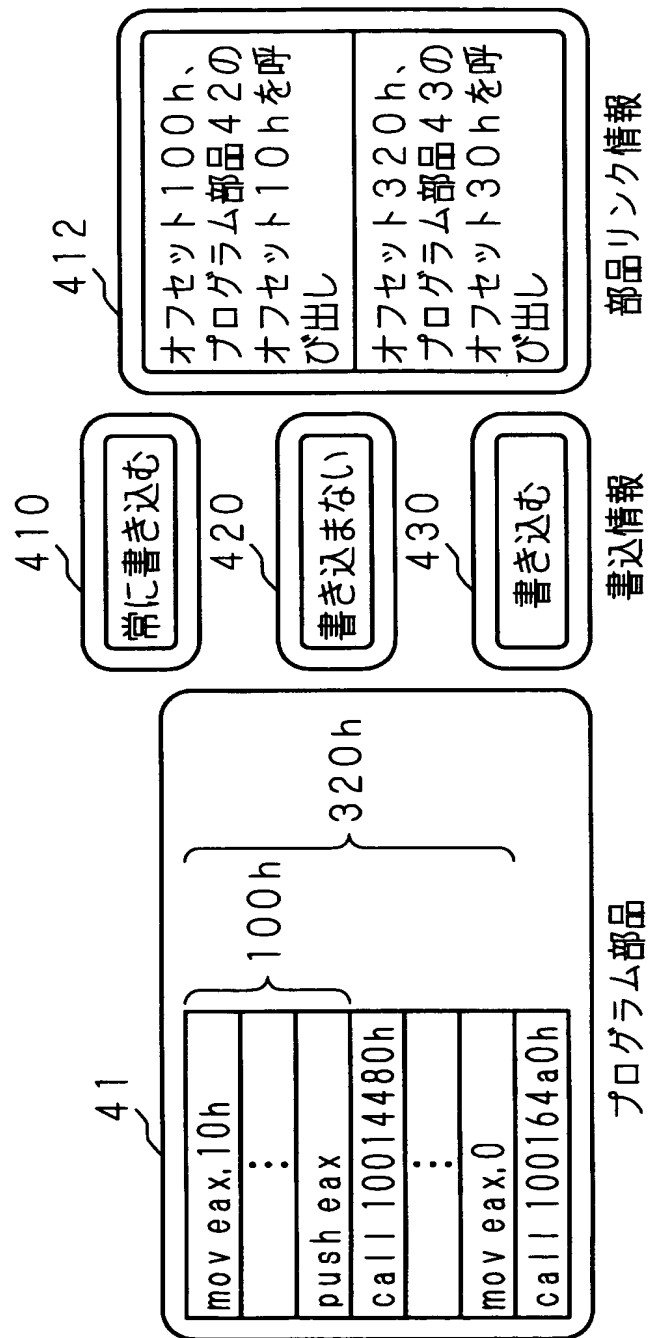
【図 12】

セキュアモジュールが行う特殊コード呼び出し処理の説明図



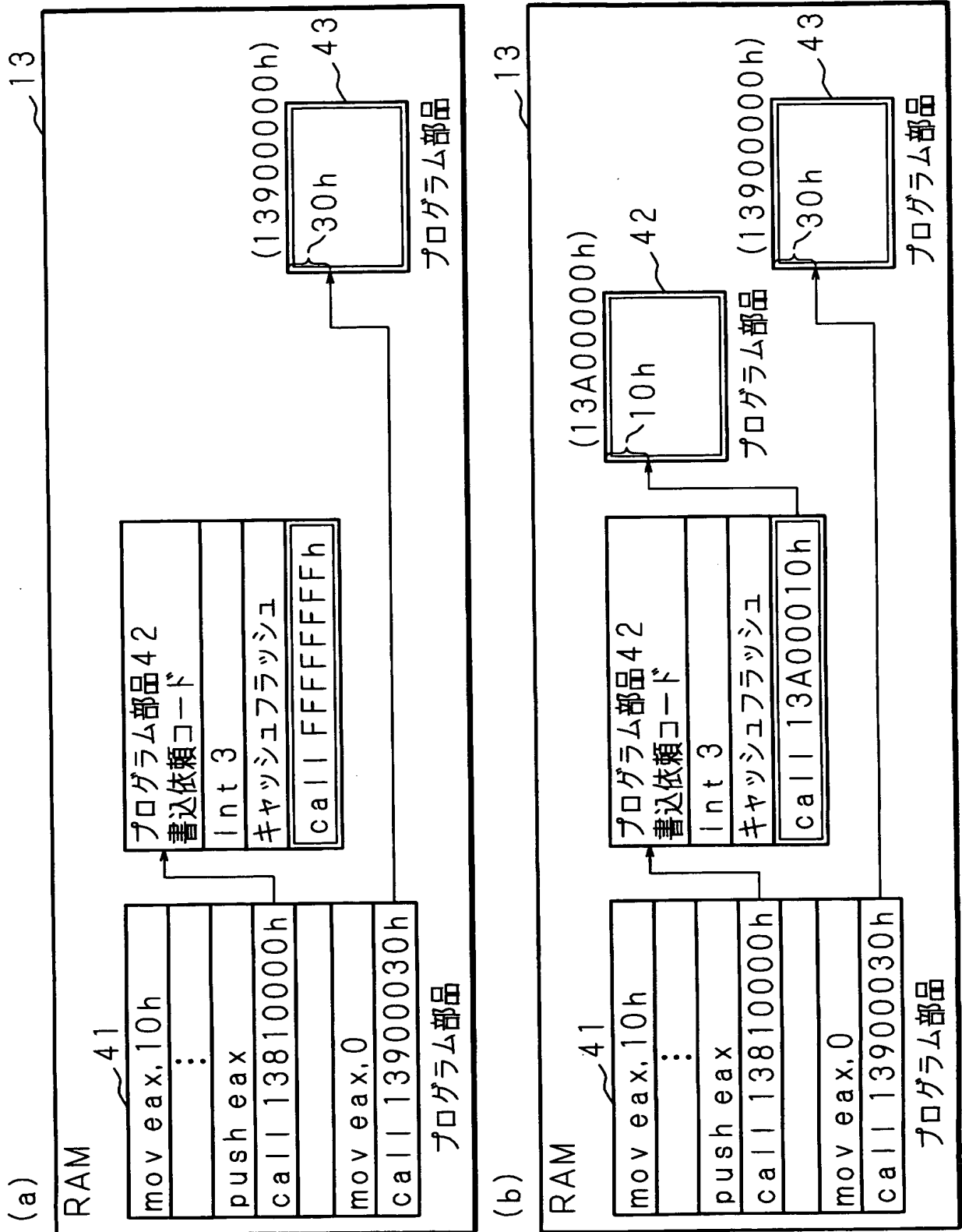
【図 13】

プログラム部品の動的書き込み処理及びリンク処理についての説明図



【図 14】

プログラム部品の動的書き込み処理及びリンク処理についての説明図



**【書類名】 要約書****【要約】**

**【課題】** プログラムを実行する場合に、悪意ある第三者による逆解析を困難にし、実行するロードモジュールの安全性を高めることができる情報処理装置を提供する。

**【解決手段】** 第1の記憶手段13と、該第1の記憶手段13に書き込まれたプログラムを実行するCPUと、セキュアモジュール20と、暗号化されたプログラムを記憶する第2の記憶手段とを有する情報処理装置において、第2の記憶手段は、複数に分割されたプログラムを記憶しており、CPUは、第2の記憶手段に記憶されたプログラムをセキュアモジュール20へ転送すべくなしてあり、セキュアモジュール20は、第2の記憶手段に記憶されたプログラムを受け取る手段と、受け取ったプログラムを実行可能な状態へ復帰させる手段と、CPUが実行する順序で、実行可能な状態へ復帰されたプログラムを第1の記憶手段13に書き込む手段と、CPUにより実行終了後に第1の記憶手段13から削除する手段とを備える。

**【選択図】**

図 5



特願 2 0 0 3 - 3 7 2 3 7 4

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 2 2 3 ]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社